Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and other Telecommunications Services	)	WC Docket No. 16-106
	)	
	)	
	)	

RESPONSE BY CONSUMER FEDERATION OF CALIFORNIA (CFC) RELATED TO THE NOTICE OF PROPOSED RULEMAKING (NPRM)

Richard Holober,
Executive Director

Carl Block,
Legal Intern

1107 9th Street, Suite 625
Sacramento, CA 95814
(916) 498-9608

CONSUMER FEDERATION OF CALIFORNIA

CFC

July 6, 2016

Introduction.

The Consumer Federation of California is pleased to submit our response to comments for consideration by the Federal Communications Commission in the above-referenced matter.

The Consumer Federation of California (CFC) is a non-profit consumer advocacy organization. In our initial comments to the FCC in this proceeding, we described the many ways in which for the past fifteen years, privacy has been a central focus of our work. We have worked extensively on legislation and regulations that protect consumer privacy, participated in the enactment of landmark California financial privacy laws and insurance and public utility privacy regulations, and led successful campaigns that stopped attempts to weaken telecommunications, medical and credit card privacy laws.

The CFC applauds the FCC's move to improve consumer privacy. The FCC has the authority to protect broadband users. Consumers must be able to protect their privacy, which requires transparency, choice, and data security. Broadband user information is sensitive, and deserves protection. Broadband Internet Access Service (BIAS) provider surveillance of consumers violates their right of privacy. BIAS providers should not be permitted to share, sell or otherwise use consumer information except to provide the consumer the broadband access service, except when a consumer elects to permit sharing in a narrow, easy to understand, revocable opt-in choice that should be presented to the consumer in such a manner that it is not perceived by the consumer as part of establishing, activating or using the service.

Since privacy is a right, we strongly urge the FCC to prohibit businesses to charge for the right. However, if the FCC disagrees and allows BIAS providers to collect and monetize surveillance information on consumers, instead of consumers' paying for privacy, BIAS providers should pay consumers for monetizing their private information. The FCC should prohibit any pay for privacy option in this proceeding, and to ensure consumers are paid a fair price for their information, in a subsequent proceeding the FCC should require BIAS providers to disclose to the FCC and to consumers their actual and projected revenues from selling or sharing private consumer information, or access to that information, and the FCC should analyze that revenue to determine a commission or royalty payment schedule for BIAS providers to pay consumers to use their information.

The FCC has the Authority to Protect Broadband Users.

The FCC has the authority to protect the privacy of broadband users. The Association of National Advertisers claimed that the "FCC is on uncertain footing for the broad and sweeping changes it proposes," because the Open Internet Order is under careful court review[1] The case cited by the Association of National Advertisers, *U.S. Telecom Association v. FCC*, was decided by the United States Court of Appeals for the District of Columbia Circuit on June 14, 2016[2]. The court rejected the argument that the FCC did not have the authority to promulgate open Internet rules.

Congress granted the FCC authority to regulate interstate communications transmitted by wire or radio in the *Communications Act of 1934*. *47 U.S. Code § 151*. Broadband Internet Access Service is a communications service provided by wire and radio in order to transmit data over the Internet; therefore, it fits within the areas that can be regulated by the FCC. *47 C.F.R. § 8.2*. When a court reviews an agency's construction of the statute that it administers, if the statute is silent or ambiguous with respect to the specific issue, the question for the court is whether the agency's answer is based on a permissible construction of the statute. *Chevron, U.S.A., Inc. v. Nat. Resources Def. Council, Inc.*, 467 U.S. 837, 842-43 (1984) (The Supreme Court reversed a lower court ruling, finding that the Environmental Protection Agency's interpretation of the Clean Air Act was a permissible construction, and entitled to deference). Therefore, the FCC's interpretation of 47 U.S.C. § 151 is entitled to deference.

Both the FCC and FTC recognize that they have authority over different parts of the Internet. The FCC regulates BIAS providers, because broadband Internet access service is provided by radio and wire, in accordance with *47 U.S. Code § 151*. The FTC has authority over Internet edge providers, under the FTC's dual mission of protecting consumers and promoting competition[3]. To that end, the FCC and FTC signed a memorandum of understanding where each

---

[1] *Comments of the Association of National Advertisers, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* pg 5.

[2] *U.S. Telecom Ass'n v. FCC*, No. 15-1063, ___ F.3d ___ (D.C. Cir. June 14, 2016), available at https://www.cadc.uscourts.gov/internet/opinions.nsf/3F95E49183E6F8AF85257FD200505A3A/$file/15-1063-1619173.pdf , accessed June 22, 2016.

[3] *What We Do*, FTC, https://www.ftc.gov/about-ftc/what-we-do, accessed 17 May 2016. *Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information*, FTC, https://www.ftc.gov/news-events/press-releases/1998/08/internet-site-agrees-settle-ftc-charges-deceptively-collecting, accessed 17 May 2016.

agency recognizes the others' area of responsibility and agreed to coordinate and consult on areas of mutual interest[4].

We do not see a reason that the FCC and FTC need to implement regulations simultaneously. The FCC is implementing regulations within its area of responsibility. We look forward to the FTC coordinating, and enacting similar regulations within their area of responsibility. It would needlessly delay protections for consumers if the government requires that the FCC and FTC implement their regulations simultaneously.

Broadband User Information Is Sensitive, and Deserves Protection.

The Association of National Advertisers wrote that the Commission cited no evidence that the non-sensitive customer information collected or shared by BIAS providers is particularly prone to unauthorized disclosure[5]. This statement is fundamentally flawed in two ways. First, it is factually incorrect. Second, the comment infers that only non-sensitive customer information would be collected.

Broadband customer information is sensitive. Unlike edge service providers, BIAS providers can view every bit of data that a broadband customer transmits across the Internet. If a broadband customer transmits medical information across the Internet, that information will be collected by the surveillance systems of BIAS providers[6]. If a broadband customer visits a lawful but embarrassing website that they do not want their family to know about, the surveillance system of the BIAS provider will capture that information. If the broadband customer uses a texting application to communicate with their friends, the surveillance system of the BIAS provider will capture that conversation. Each of these scenarios represents information that is sensitive to a consumer. Each of these scenarios can cause real harm to a consumer.

---

[4] *Memorandum of Understanding on Consumer Protection Between the FTC and the FCC*, November 16, 2015, available at https://www.ftc.gov/policy/cooperation-agreements/memorandum-understanding-consumer-protection-between-federal-trade, accessed 15 May 2016.

[5] *Comments of the Association of National Advertisers, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, pg 10.

[6] *ZephyrLIFE Home Remote Patient Monitoring*, available at http://www.medtronic.com/covidien/products/health-informatics-and-monitoring/zephyr-life-home-remote-patient-monitoring, accessed June 22, 2016.

Medical information is protected by law because of its sensitive nature[7]. Information about lawful, embarrassing websites could permanently damage a person's family relationships. Information from captured text and email conversations could also damage a person's family, friend, or business relationships. It is flawed logic and a misstatement of fact to argue that the FCC should not act to protect consumer information because there has not been a previous unauthorized disclosure of surveillance information from a BIAS provider. In 2015, BIAS provider Comcast paid $33 million to settle a California Public Utilities Commission complaint that it had published the phone numbers of 74,000 California consumers who had paid an extra fee of $1.25 to $1.50 a month to unpublish their Voice over Internet Protocol (VOIP) phone numbers.[8] These broadband customers had paid for a unique aspect of Internet privacy related to a telecommunications service that Comcast bundles with its "Xfinity" broadband access service. Comcast states in its online marketing materials: "VoIP and XFINITY - Voice over Internet Protocol (VoIP) is a technology used to transmit voice and related calls over a data network. Most VoIP service providers use the public Internet to transmit your calls. We don't – we transmit your calls over our own advanced broadband network."[9]

Violating its contractual agreement with these customers, this BIAS provider published their unlisted phone numbers. In its defense, Comcast essentially stated that it had "goofed" by not placing a privacy flag on these consumers' phone numbers before sharing them with a third party phone publisher of its phone directory.[10] Further, the inaccurate statement that there has not been an unauthorized disclosure of "non-sensitive" information in the past assumes that BIAS consumers have had the choice to "authorize" or withhold authorization of the disclosure of their information. In the unusual circumstance of VOIP service, where a "pay for privacy" standard

---

[7] *Health Insurance Portability and Accountability Act of 1996*, PL 104-191, August 21, 1996, 110 Stat 1936.

[8] Attorney General Kamala D. Harris Reaches $33 Million Settlement With Comcast Over Privacy Violations, September 17, 2015, available at https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-reaches-33-million-settlement-comcast-over, accessed July 1, 2016.

[9] https://customer.xfinity.com/help-and-support/internet/voice-over-internet-protocol/, accessed July 6, 2016/

[10] Ashlee Kieler, *Comcast Must Pay $33M To Settle Charges It Listed 75,000 Unlisted Phone Numbers*, The Consumerist, September 18, 2015, available at https://consumerist.com/2015/09/18/comcast-must-pay-33m-to-settle-charges-it-listed-75000-unlisted-phone-numbers/, Accessed July 1, 2016.

applies to phone directories, BIAS provider Comcast committed an unauthorized disclosure of individually identifiable consumer information. In most circumstances, BIAS consumers have lacked the right to tell a BIAS provider that they are not authorizing the disclosure of their information. Unless consumers can withhold authorization, which in most cases they cannot, it is not possible to discern whether or not BIAS providers are disclosing information under authorization-free business practices.

Unauthorized disclosures can occur through BIAS provider error, as in the Comcast example, and through lapses in security. As BIAS providers collect more and more consumer information, their database becomes more and more valuable. Hackers are becoming more sophisticated every day, and have proven their ability to exfiltrate information from protected computer systems[11]. Because hackers are becoming more sophisticated, and the databases are becoming more valuable targets, one cannot infer that there will not be more unauthorized disclosures in the future.

Even if there is never again an unauthorized disclosure of private information, the information still should not be collected by BIAS providers. Surveillance of broadband consumers gives BIAS providers unparalleled access to the intimate details of consumer behavior and communications. BIAS providers collect all of the information a consumer sends over the network[12]. BIAS providers can see who communicates with whom. BIAS providers can see all of the information people send via email, text, or snapchat. The massive details that BIAS providers could collect would dwarf the information that Edward Snowden recently disclosed was collected by the National Security Agency (NSA). The NSA only collected

---

[11] Nicholas Percoco, *Data Exfiltration, How Data Gets Out*, Computer World, Mar 12, 2010, available at http://www.computerworld.com/article/2520483/enterprise-applications/data-exfiltration--how-data-gets-out.html, accessed June 22, 2016.

Tom Vanden Brook and Michael Winger, *Hackers Penetrated Pentagon Email*, USA Today, Aug 7, 2015, available at http://www.usatoday.com/story/news/nation/2015/08/06/russia-reportedly-hacks-pentagon-email-system/31228625/, accessed June 22, 2016.

[12] Super Cookies are one method of collecting information about consumers via their mobile network, as shown in *The Rise of Mobile Tracking Headers: How Telcos Around the World are Threatening Your Privacy*, Access, available at https://www.ftc.gov/system/files/documents/public_comments/2015/09/00008-97486.pdf, accessed June 30, 2016.

telephone call meta-data, such as which number was called[13]. A BIAS provider can collect information about who the consumer communicated with, plus the intimate details of the email, text or snapchat conversation.

The FCC's Proposed Rule Does Not Violate the 1st Amendment, instead, BIAS Provider's Surveillance of Consumers Violates the Right of Privacy.

The Association of National Advertisers claims that that FCC rule constitutes a restriction on commercial speech, tailored to a particular audience[14]. The FCC rule does not restrict speech, because advertisers can continue to advertise to consumers in a manner that balances consumers' privacy rights with the commercial interests of advertisers and BIAS providers. The FCC rule does restrict the ability of BIAS providers to collect private information from consumers.

The act of collecting private information is not speech, and is therefore not protected under the First Amendment. Speech involves words or conduct that expresses opinions or thoughts[15]. The act of collecting private information does not involve words that express opinions or thoughts of the person or organization collecting the information. The act of collecting private information is conduct; however, it is not conduct that expresses the opinions or thoughts of the person or organization collecting the information. Therefore, collecting private information is not speech protected under the First Amendment.

On the other hand, even if the government finds that collecting private information is a form of speech, the government is still authorized to regulate the speech because it is commercial speech. The constitution accords less protection to commercial speech than to other constitutionally safeguarded forms of expression[16]. The government is authorized to regulate commercial speech if the state has a substantial interest to be achieved by restrictions on

---

[13] Adriane de Vogue, *Court Rules NSA Program Illegal*, CNN, May 7, 2015, available at http://www.cnn.com/2015/05/07/politics/nsa-telephone-metadata-illegal-court/, accessed June 22, 2016.

[14] Comments of the Association of National Advertisers, In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, pg 31.

[15] *Black's Law Dictionary* (Bryan A. Garner, Ed., 9th Ed. 2010).

[16] *Bolger v. Youngs Drug Prods. Corp.*, 463 U.S. 60, 64 (1983).

commercial speech, and if the regulatory technique is in proportion to that interest[17]. The government has a substantial interest in restricting the collection of private information because privacy is a right.

The Supreme Court has long identified a right to privacy against the government. In *Griswold v. Connecticut*, the Court held that the first amendment has a penumbra whereby privacy is protected from governmental intrusion[18]. The Court later clarified the definition, when it stated that privacy includes an individual interest in avoiding disclosure of personal matters[19]. The Court later extended the definition, when it recognized that "the zone of privacy long has been held to encompass an "individual interest in avoiding disclosure of personal matters."[20] The Court has recognized that "the outer limits of this aspect of privacy have not been marked by the Court."[21]

State constitutions and common law have helped to further define the right of privacy. Privacy torts have been judicially recognized or statutorily enacted in almost every state. In addition, at least ten states have recently enshrined the right of privacy into their constitutions[22]. In California, one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person[23].

---

[17] *Central Hudson Gas and Electric Corp. v. New York Public Service Commission*, 447 U.S. 557, 564 (1980).

[18] *Griswold v. Connecticut*, 381 U.S. 479, 483 (1965).

[19] *Whalen v. Roe*, 429 U.S. 589, 599 (1977). The Court wrote "The cases sometimes characterized as protecting "privacy" have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."

[20] *Ohio v. Akron Ctr. for Reprod. Health,* 497 U.S. 502, 529 (1990)

[21] *Carey v. Population Services, Intern.,* 431 U.S. 678, 684 (1977)

[22] Matthew C. Keck, *Cookies, the Constitution, and the Common Law: A Framework for the Right of Privacy on the Internet*, 13 Alb. L.J. Sci. & Tech. 83, 105 (2002).

[23] *Shulman v. Group W Productions, Inc.*, 955 P.2d 469, 490 (Cal. 1998), as modified on denial of reh'g (July 29, 1998).

Physical intrusion is not required. The key question is whether the a reasonable consumer believes it is highly offensive that a BIAS provider monitors all of their web traffic, email, tweets, and other Internet communications, and then shares that information, or access to that information, with advertisers and other third parties.

Our contention is that a reasonable consumer is unaware of the degree to which BIAS providers can monitor all of their web traffic. When consumers become aware of the degree they are monitored by BIAS providers, they will find the monitoring highly offensive. Monitoring by BIAS providers is similar to, but more intrusive than, when Google monitors email accounts. When consumers learned that Google was monitoring their email accounts, and sending them advertisements based on the email communications, consumers fought back. In 2014, Google bowed to pressure and promised to stop monitoring student email accounts[24]. But Google continued to monitor email accounts after the promise, so Google was sued in February 2016 for breach of the Electronic Communications Privacy Act[25]. If consumers found Google monitoring offensive, they will also find the more intrusive BIAS provider monitoring Offensive.

BIAS Provider's Surveillance of Consumers Erodes 4th Amendment Protections.

The Fourth Amendment protects an individual's privacy from Government intrusion. Under *Katz v. United States,* the Supreme Court specified a twofold rule for the protection of a person's privacy against government surveillance[26]. First that a person have exhibited an actual (subjective) expectation of privacy, and second that the expectation be one that the society is prepared to recognize as "reasonable." The issue here is that ubiquitous commercial surveillance, as implemented by BIAS providers, leads consumers, and society in general, to feel thee is no actual privacy on the Internet[27]. If people feel that there is no privacy on the Internet,

---

[24] Juan Carlos Perez, *Google Stops Scanning Gmail Messages for Ads in Apps for Education*, PC World. Available at http://www.pcworld.com/article/2149960/google-stops-scanning-gmail-messages-for-ads-in-apps-for-education.html, accessed June 19, 2016.

[25] *Casey Sullivan, Google Sued (Again) for Scanning University Emails*. Findlaw.com, Available at http://blogs.findlaw.com/technologist/2016/02/google-sued-again-for-scanning-university-emails.html, Accessed June 19, 2016.

[26] *Charles Katz v U.S.*, 389 U.S. 347, 361 (1967).

[27] Mary Graw Leary, *Katz on A Hot Tin Roof-Saving the Fourth Amendment from Commercial Conditioning by Reviving Voluntariness in Disclosures to Third Parties*, 50 Am. Crim. L. Rev. 341, 343 (2013)

then, under the Katz rule, a person does not have an actual expectation of privacy. If people do not have an expectation of privacy, then the government may lawfully perform surveillance on the Internet under the 4th Amendment, because there is no reasonable expectation of privacy. Although a case has yet to come before the Supreme Court to test the actual expectation of privacy in an era where BIAS providers can monitor every action of a consumer on the Internet, it is reasonable to see how allowing BIAS providers to monitor actions on the Internet erodes privacy under the 4th Amendment.

Privacy is a Right, therefore, the FCC Should Not Allow Businesses to Charge for the Right.

As shown above, privacy is a right. We recommend that the FCC not allow business to charge for the right to privacy. We also recommend that the FCC not allow financial inducements for privacy.

AT&T has offered customers a discount of roughly $30 per month if they allow AT&T to track and use their individual web browsing information in order to tailor ads and offers to the customers' interests. Another way to think of the AT&T offer is that consumers who want privacy have to pay $30 extra per month, or $360 per year, as opposed to those who do not get privacy. Other businesses are eager to roll-out a similar programs[28]. Verizon, AT&T, Sprint and T-Mobile are collecting consumer information from their mobile and fixed networks in order to derive income from advertisers by targeting ads more effectively[29].

The major telecommunications companies are not collecting consumer information because they are benevolent. Consumer behavior information is extremely valuable[30]. The BIAS providers will make money by sharing consumer information for advertising purposes. They also make money by charging the consumer for privacy, if the consumer is unwilling to allow the BIAS provider to snoop into their private information that is transmitted over the network. Either way, the BIAS providers win, and the consumer loses.

---

[28] Stacey Higginbotham, *ISPs really, really want to be able to share your data*, Forbes, (Apr 28, 2015), available at http://fortune.com/2015/04/28/isps-share-your-data/, accessed 15 May 2016.

[29] Adam Cohen-Aslatei, *Telcoms Open Shop on Madison Avenue, But Will Brands Buy?*, TechCrunch, 25 June 2016, available at https://techcrunch.com/2016/06/25/telecoms-open-shop-on-madison-avenue-but-will-brands-buy/, accessed June 30, 2016.

[30] Telecommunications companies are battling over customer data that powers the $100 billion global mobile advertising industry. *Id*.

A fundamental problem with AT&T charging $360 per year for not monitoring and recording consumer web traffic is that only the wealthiest consumers will be able to afford privacy. The poor and working families living paycheck to paycheck will never be able to afford privacy.

The "digital divide" is an economic and social inequality with regard to access to the Internet[31]. The "digital divide" was first identified over a decade ago, and continues today[32]. The Pew Research Center identified that cost continues to be a significant factor for Americans who do not have access to the Internet[33]. Research shows that Americans hold strong views about online privacy[34]. The difficulty consumers face is that most consumers struggle to place a monetary value on privacy. BIAS providers are taking advantage of the consumer's difficulty in understanding the value of privacy. By charging for privacy, BIAS providers are increasing the digital divide in the area of privacy. Only the wealthiest and most astute consumers will choose to afford the right of privacy. The poor, working families, and those living on fixed incomes will not be able to afford the right of privacy.

If the FCC Does Not Protect the Right of Privacy, then the FCC Should Require Consumers to be Paid for Their Private Information.

We urge the FCC to prohibit any scheme that permits a BIAS provider to offer a financial incentive to a consumer for waiving privacy, or a penalty or disadvantage for asserting the right to privacy. Alternatively, should the FCC consider any pay for privacy proposal, we urge that it not occur in this proceeding, but in a subsequent proceeding in which the FCC first determines the value to the BIAS provider for sharing consumer information, and then develop a schedule in

---

[31] *Digital Divide*, Wikipedia, available at https://en.wikipedia.org/wiki/Digital_divide, accessed 22 May 2016.

[32] Council of Economic Advisors Issue Brief, *Mapping the Digital Divide*, July 2015, available at https://www.whitehouse.gov/sites/default/files/wh_digital_divide_issue_brief.pdf, accessed on 22 May 2016.

[33] Pew Research Center, *Digital Divides 2015*, September 22, 2015, http://www.pewinternet.org/2015/09/22/digital-divides-2015/, accessed on 22 May 2016.

[34] Marry Madden and Lee Rainie, *Americans' Attitudes about Privacy, Security and Surveillance*, Pew Research Center, May 20, 2015, available at http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/, accessed May 22, 2016.

which BIAS providers would be required to pay their customers a commission or royalty payment reflecting the value of the information that the consumer owns and that the BIAS provider shares with third parties in return for receiving a payment or other consideration.

Rather than permitting BIAS providers to require consumers to pay for privacy, any future FCC consideration of this issue should start with the premise that a BIAS provider collects consumer information for the limited purpose of providing the consumer a high speed Internet connection, and that it should pay a consumer a fair value when it derives income for other uses of consumer information. BIAS providers put a monetary value on the private information of consumers[35]. Consumers are challenged because they do not know how much their private information is worth. Perhaps some consumers may be willing to permit a BIAS provider to monetize their personal information if the BIAS provider pays them a fair value. The FCC does not have adequate information to evaluate the present and projected future monetary worth of consumer information. To resolve the situation, should the FCC disagree with our view that privacy is a right that should not have a price tag, we propose that BIAS providers and others disclose the revenue they make, and project to make, from consumers' private information. Armed with this information, the FCC should require BIAS providers to pay consumers a reasonable percentage, perhaps 80% or 90%, or more, of the revenue that they receive from consumers who opt-in to permit the use of their private information. Any consideration of this concept should occur in a subsequent FCC proceeding. In the current proceeding the FCC should ban any pay for privacy options.

Some consumers may be willing to opt-in and share their private information if they receive sufficient value in return. In January 2016, the Pew Research Center released a study of consumer perceptions of privacy and information sharing[36]. The study surveyed 461 U.S. adults, presenting them with six different information sharing or surveillance scenarios. None of the scenarios matched the intrusive capability of a BIAS provider to monitor every website a consumer visits, and every email or tweet that a consumer sends or receives. Nonetheless, the scenarios reveal that consumer's willingness to share information about themselves is contingent upon the circumstances of the offer, their trust of those collecting and storing the data, and their sense of how the data might be shared. In the Pew study, the scenario that was closest to a BIAS provider's monitoring was described as a social media platform that people could voluntarily visit to find out information about a class reunion; however, the social media

---

[35] Brian Fung, *How much is your privacy worth? $350 a year, according to AT&T*, The Washington Post, December 11, 2013, available at https://www.washingtonpost.com/news/the-switch/wp/2013/12/11/how-much-is-your-privacy-worth-350-a-year-according-to-att/, accessed June 21/2016.

[36] Lee Rainie and Maeve Duggan, *Privacy and Information Sharing*, Pew Research Center, January 14, 2016, available at http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/, accessed June 21, 2016.

company would monitor the consumer's use of the website in order to deliver targeted advertisements to the consumer. Over half (51%) of all study participants found this monitoring unacceptable. One third, (33%) were willing to accept the monitoring in this scenario. It is interesting to note that 17% of adults said they would not accept any of the deals offered in any of the six scenarios.

BIAS providers have placed a monetary value on consumers' private information. AT&T is offering consumers an inducement of $30 per month, or $360 per year; therefore, it is highly likely that AT&T believes they can sell or share access to an individual consumer's information for as much as $360 per year[37]. Consumers do not know how much their private information is worth. Academic research suggests that a consumer's perception of the value of privacy is highly malleable, and subject to how the question is asked[38].

Because BIAS providers know the value of private information, and neither consumers nor the FCC knows the value of their private information, we propose that the FCC help make the deal fair for consumers. Before the FCC were to take any action other than to prohibit any pay for privacy options, the FCC needs to gather information regarding the revenues or other considerations that BIAS providers receive from information sharing. We propose that BIAS providers report to the FCC and the public how much revenue they receive, and project to receive, from selling or sharing access to consumers' private information. The FCC can then establish a fair percentage of the revenues they receive that BIAS providers would then pay consumers who chose to opt-in. Using this simple method, consumers can understand the value of their private data, and will be assured that they are receiving a fair payment when they elect to allow a BIAS provider to collect and share their private information.

We believe that gathering and disseminating this information would advance the public's understanding of the monetization of private information that the overwhelming majority of Americans believes should not be collected or shared without their consent. The likely result would be an increase in public outcry against profiteering from these privacy intrusions.

---

[37] Stacey Higginbotham, *ISPs really, really want to be able to share your data*, Forbes, (Apr 28, 2015), available at http://fortune.com/2015/04/28/isps-share-your-data/, accessed 15 May 2016.

[38] Alessandro Acquisiti, Leslie John, and George Loewenstein, *What is Privacy Worth?*, available at http://www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-worth.pdf, accessed June 21, 2016.

Conclusion.

The Consumer Federation of California applauds the FCC's step forward to improve consumer online privacy. The FCC has the authority to promulgate rules to protect the privacy of consumers. Privacy is a right. Because it is a right, it should be protected. Consumers should not pay to assert this right. We strongly urge the FCC to ban any pay for privacy regulation. However, if the FCC does not protect this right, then the FCC should require BIAS providers to pay consumers for the sale or sharing of their private information. Because regulators and consumers do not know the monetary value of their private information, in a subsequent proceeding, the FCC should require BIAS providers to disclose the revenue they receive for selling or sharing the information, and, adopt regulations requiring BIAS providers to pay consenting consumers a reasonable percentage of the revenue they receive.